Reznick Group

MANAGEMENT LETTER

CITY OF ROCKVILLE, MARYLAND

JUNE 30, 2009

Reznick Group

Reznick Group, P.C.
500 East Pratt Street
Suite 200
Baltimore, MD 21202-3100

Tel: (410) 783-4900
Fax: (410) 727-0460
www.reznickgroup.com

October 30, 2009

To The Honorable Mayor, Members of the City Council and City Manager
City of Rockville, Maryland

Ladies and Gentlemen:

In planning and performing our audit of the financial statements of City of Rockville, Maryland (the City), we considered the City's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. We refer you to our Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards dated October 30, 2009, our Report on Compliance with Requirements Applicable to Each Major and Nonmajor Program and Internal Control Over Compliance in Accordance with OMB Circular A-133 dated October 30, 2009. We did become aware of a few matters that are opportunities for strengthening internal controls and operating efficiency. We offer the following comments for your consideration:

Segregation of Duties

Observation:

The City should segregate the duty of printing the payroll checks from the Information Technology department. The payroll department should have the ability to print the payroll checks without any assistance from the Information Technology department.

Risk:

The Information Technology department could override the controls in place with regard to the payroll software.

Management Response:

The printing of payroll has been segregated to the Payroll Department. This became effective in August 2009. The Payroll Department has sole access and responsibility to print payroll checks.

Access Controls

Observation

1. There are shared user accounts for the network and for database access.

2. Access to the network is not reviewed quarterly.

3. The Novell password parameters are weak as Novell enforces password parameters which do not follow industry standards.

Risk

1. When (user or admin) accounts are shared, there is a lack of accountability as changes cannot be traced back to the individual who made the changes.

2. Without a review of network users' access, access to files and other system resources may not be in line with their job functions.

3. The password policy as stated is not very strong and increases the risk of unauthorized or erroneous access to the network.

Recommendation

1. Management should remove shared accounts if possible and assign individual accounts so that each user is accountable for their actions.

2. Management should consider reviewing network users on a quarterly basis.

3. Management should consider enhancing the password policies in Novell to provide stronger authentication controls to the network. (The client stated that they are migrating to Active Directory and plan to enforce stronger password parameters.)

Management Response

1. Shared network accounts have been eliminated. Shared database access is limited to the two system administrators who administer the financial system database. IT staff is currently working with the Finance Department to upgrade the financial system to a newer version, at which time the shared database access will be eliminated. The upgrade is scheduled to be completed in Fall 2009.

2. The client provided evidence that they had performed a review of network access while the auditors were onsite, August 28, 2009. IT staff plan to review network access on a quarterly basis.

3. Network password requirements have been expanded to industry standard levels and were fully implemented on October 20, 2009.

Security Policies and Procedures

Observation

Policies and procedures are in the draft form for information security; access controls, including a password policy; and physical security.

Risk

Documented policies and procedures help ensure consistent execution of management's intentions, enforce compliance, facilitate training, serve as a daily reference, and can be used to help measure individual performance. Without documented policies and procedures, there can be delay and loss of productivity in case of emergency or absence of staff, particularly in smaller departments.

Recommendation

Management should complete their security policies and procedures and disseminate them for use.

Management Response

IT staff will be revising the draft policy and procedures and expects to have final documents completed well before the end of FY10.

Change Management

Observation

There is not a documented change management/patch update policy.

Risk

Without a documented policy, it is more difficult to ensure that procedures are followed each time a change is made.

Recommendation

Management should consider documenting the change management policy that includes patch updates to systems. The policy should address authorization, testing, approval and proper implementation of changes.

Management Response

A formal change management policy is under development and is expected to be completed and implemented well before the end of FY10.

Conclusion

Reznick Group offers the preceding comments for your review and consideration. We have already discussed many of these comments with various City personnel, and we will be pleased to discuss them in further detail at your convenience. We appreciate the courtesies extended to us during our engagement by the City's personnel and look forward to a continued mutually beneficial relationship.

This letter is intended solely for the information and use of the City's management and the City Council and is not intended to be and should not be used by others.

Very truly yours,

Reznick Group, P.C.

Reznick Group, P.C.